CITY OF ISSAQUAH

ADMINISTRATIVE MANUAL

Code #: 101-26	
Index: ADMINISTRATION AND POLICY MANAGEMENT	

Title: TECHNOLOGY RESOURCE USAGE & SECURITY POLICY

Effective Date:	**Supersedes:**		**Page:** 1	**Of:** 11
03-18-2019	06-01-2010			

101-26-01 PURPOSE

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at the City of Issaquah. The purpose of these policies is to safeguard and protect all technology resources from anything other than authorized and intended use. The main points are:

1. The City provides computing and network resources ('technology') to carry out legitimate City business.

2. There is no right to privacy in the use of City technology resources.

3. Users are expected to act lawfully, ethically and professionally, and to exercise common sense. Actions that are embarrassing to explain to the public, Mayor, City Council, or media should be avoided.

4. Users granted access to critical data are responsible for its protection.

5. Incidental use for personal needs is allowed as long as that activity does not interfere with City business or conflict with any City policy or work rule.

6. Use of technology in violation of this policy is subject to disciplinary action, up to and including, termination of employment.

101-26-02 GROUPS AFFECTED:

This policy applies to all City of Issaquah offices, departments, elected officials, employees, consultants, contractors, volunteers, and system users, or anyone who has access to any form of a city-owned computer, network, or application account.

101-26-03 REFERENCES:

Payment Card Industry (PCI) Data Security Standard, PCI Security Standards
Council Washington State Patrol A Central Computerized Enforcement Service System (ACCESS) Triennial Audit Packet, Washington State Patrol

101-26-04 POLICY:

A. Scope

The following policies define appropriate use of the City of Issaquah network, computers, all related peripherals, software, electronic communications, and Internet access. These policies apply to the access of the City's network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all users of City technology resources regardless of employment status. Access to all networks and related resources require that each user be familiar with these policies.

The City of Issaquah authorizes the use of computing and network resources by City staff, elected officials, contractors, volunteers and others to carry out legitimate City business. All users of City computing and network resources will do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules. Technology resources may not be used to facilitate operation of a personal business, such as sale of cosmetics or consulting. Staff will approve and post approved listings for services, items for sale, and/or wanted items in the Classified Section of the Employee Intranet.

B. Ownership of Data

The City owns all data stored on its network and systems (including e-mail, voicemail and Internet usage logs) and reserves the right to inspect and monitor any and all such communications at any time, for any business purpose, with or without notice to the employee. The City may conduct random and requested audits of employee accounts in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, and to assist Departments in evaluating performance issues and concerns. Internet and e-mail communications may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The City's Internet connection and usage is subject to monitoring at any time with or without notice to the employee. There is no right to privacy in the use of City technology resources.

C. Personal Use

Technology resources may be used for incidental personal needs as long as such use does not result in or subject the city to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City's reputation or credibility, or conflict with the intent or requirements of any City policy or work rule. Personal usage should generally conform to limits typically associated with personal phone calls. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense should be exercised while using City technology resources. This document provides policies and general rules for appropriate use of resources. Staff use of technology resources in violation of this policy or otherwise inappropriate technology resource usage is subject to disciplinary actions up to and including termination of employment.

1. Applicability

1.1. This policy applies to all City of Issaquah offices, departments, elected officials, employees, volunteers, and system users.

2. Security Management

2.1. All suspected information security incidents must be reported as quickly as possible through management to the Information Technology Office.

2.2. Responsibility for Information Security.

2.2.1. All major data systems must have a designated Owner. Owners make decisions about who will be permitted to access information, and the uses to which this information will be put. Owners should additionally take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information. Owners will normally be the director of the department with the major interest in the data system.

2.2.2. All major data systems will have a designated Security Administrator to define user privileges, monitor access control logs, and perform similar security activities. The Security Administrator will normally be designated by the owner of the of data system.

2.3. Unless specifically authorized in writing, by the Information Technology Manager, hardware or software tools will not be used that could evaluate or compromise information security systems.

3. Access Control

3.1. User Access Privileges

3.1.1. City of Issaquah management maintains the authority to: (1) restrict or revoke any user's privileges, (2) inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and (3) take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users. City of Issaquah disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

Reason: City of Issaquah uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems.

3.1.2. Each Department will designate specific employees who have authority to request accounts to be created or modified for employees.

3.1.3. Users must read the Acceptable Use Addendum and sign a User Agreement prior to being given a user-ID allowing access to City of Issaquah systems.

3.1.4. Each Department must promptly report all significant changes in end-user duties or employment status to the IT Office so that accounts and network access can be disabled for personnel that are no longer employed or requiring access.

3.1.5. On a routine basis, the ITO will compare active network accounts with a list of active employees obtained from either the Payroll or Human Resources Departments.

3.1.6. Network access accounts that have been inactive for 90 days are automatically disabled. Exceptions may be requested by Departments.

3.1.7. When a worker leaves any position within the City of Issaquah, computer resident files should be promptly reviewed by his or her immediate manager to determine who should become the custodian of such files, and/or the appropriate methods to be used for file disposal. The computer user's manager should then promptly reassign the computer user's duties as well as specifically delegate responsibility for information formerly in the computer user's possession. The system security administrator removes or restricts access as appropriate.

3.1.8. Unless Systems Security Administration has received instructions to the contrary, four weeks after a worker has permanently left the City of Issaquah, all files held in that user's directories should be archived.

3.2. Passphrases for network security

3.2.1. Access to Issaquah networks will use passphrase construction.

3.2.2. Passphrase construction, lifecycle and re-use parameters will be based on Access Type according to the classification of the system or data that these user types have access to.

3.2.3. Users will be notified one week in advance of passphrase expiration.

3.2.4. The City of Issaquah will use technical measures to ensure that users conform to the policy.

3.2.5. All passphrases must conform to the guidelines outlined below.

Access Type	Passphrase Length	Reset Frequency	Complexity
General user accounts	16	12 months	None
Police Department user accounts	16	90 days	None
Senior Leadership (Mayor, Executive office and Directors)	16	12 months	None
Finance staff	16	12 months	None
Human Resources staff	16	12 months	None
Information Technology Team staff	16	12 Months	None
Network, Server and Desktop Administrator accounts	25	12 months	None
System accounts for machine to machine	50	Never	Random string of characters

3.3. Passwords (general)

In cases where passwords are required, the following policies apply.

3.3.1. All passwords must have at least the number of characters as indicated in table in section 3.2.5.

3.3.2.

3.3.3. Passwords shall not be a dictionary word or proper name.

3.3.4. Passwords must not contain or be the same as the UserID.

3.4. Passphrase and password administration

3.4.1. Passphrases and Passwords must not be written down and left in a place where unauthorized persons might discover them.

3.4.2. Regardless of the circumstances, passphrases and passwords must never be shared or revealed to anyone else besides the authorized user or authorized IT staff during in-person support visits. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms.

3.4.3. Use of another person’s account or attempt to capture passphrases or passwords is prohibited, except for authorized IT staff during in-person support calls that are monitored by user.

3.4.4. Each user is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended.

3.4.5. The length of passphrases and passwords will be checked automatically at the time that users construct them.

3.4.6. The display and printing of passphrases and passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

3.4.7. Users must be automatically forced to change their passwords at least once per period as indicated in the table in section 3.2.5.

3.4.8. To allow passwords to be changed when needed, passphrases and passwords must never be hard-coded (programmed) into software developed by or modified by City of Issaquah workers.

3.4.9. All vendor-supplied default passphrases and passwords should be changed before any computer or communications system is used for City of Issaquah business.

3.4.10. The number of consecutive attempts to enter an incorrect passphrases or password must be limited. After five unsuccessful attempts to enter a passphrase or password, the involved UserID must be either (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than 60 minutes, or (c) if dial-up or other external network connections are involved, disconnected.

4. Application and System Development

4.1. Prior to being placed into production use, each new or significantly modified/enhanced business application system must include a brief security impact statement.

4.2. City of Issaquah production data and production computer programs must be changed only by authorized people according to established practices.

5. Operational Security

5.1. IT Office must authorize all access to central computer systems. Each user is responsible for establishing and maintaining a passphrase or password that meets City requirements. If you discover unauthorized use of your account, immediately report the unauthorized access to your supervisor and to the IT Office.

5.2. The City of Issaquah will take the necessary steps to protect the confidentiality, integrity, and availability of all of its critical information. Critical information is defined as information which if released could damage the City financially; put staff at risk; put facilities at risk; or could cause legal liability. Examples of critical data include but are not limited to: employee health information, social security numbers, credit card holder information, banking information, and police crime investigation information.

5.3. Staff with access to critical information are responsible for its protection. Staff must take reasonable steps to ensure the safety of critical information including: encrypting data any time it is electronically transported outside the City network; ensuring that inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it.

5.4. The City will restrict access to critical information only to staff that have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and ensuring that access to it is limited.

5.5. All critical data must be fully backed to tape at least weekly, preferably daily. The backup tapes must be stored off site in an environmentally protected and access controlled location.

5.6. A virus scanner must be installed on all production servers and workstations and the virus scanner must be updated at least weekly, preferably daily. Non-City of Issaquah staff (e.g. vendors, contractors) are not allowed to connect non-city equipment to the City of Issaquah network. Representatives of the contracting departments are responsible for assisting their contractors to engage the IT Office to for IT services for them to complete contracted work.

6. Network Security

6.1. The internal addresses, configuration, and related system design information for City of Issaquah networked computer systems must be restricted such that both systems and users outside the internal network could not access this information without explicit management approval.

Example: involving the Internet, the Internet protocol (IP) addresses of internal computers must be translated and concealed at a firewall, router, gateway, or at other access points.

6.2. All connections between City of Issaquah internal networks and the Internet (or any other publicly-accessible computer network) must include an approved firewall and related access controls.

6.3. When users access city systems from outside city facility networks, they must use Multi Factor Authentication for primary third-party cloud applications (such as Office 365) or for VPN (Virtual Private Network) connection to assets inside the city firewall (such as the file server) using one of the following methods:

- Receive texts on their mobile device containing a PIN which they input to gain access;
- Receive authentication approval requests on the Microsoft Authenticator app on their personal smartphone;
- Have a USB key that they plug into their desktop or laptop PC prior to inputting their account name and passphrase;
- Have an RFID tag on their employee ID badge that is read by their laptop or PC.

6.4. A connection between City of Issaquah systems and computers at external organizations, via any network, must be encrypted and approved by the IT Manager.

6.5. Before a connection between the City of Issaquah network and an external organization is established, the external organization must agree to abide by all City of Issaquah security policies and standards.

6.6. User must not connect personal or non-city owned equipment, wireless access points, routers or switches, computers, servers and telephones to existing internal networks, or other multi-user systems for communicating information without the specific approval of the Information Technology Manager.

Reason: This practice will help ensure that all City of Issaquah networked systems have the controls needed to prevent unauthorized access.

6.7. Employees must not connect modems to workstations that are also connected to a local area network (LAN).

6.8. Users must not leave modems connected to personal computers in auto-answer mode, so that they are able to receive incoming dial-up calls.

7. Physical Security

7.1. Facilities which house City of Issaquah computer rooms, network centers, telecommunications controlled areas, and work areas containing sensitive data must be protected with physical security measures to prevent unauthorized access.

7.2. City of Issaquah computer rooms, network or communication centers, and other computer controlled areas (hardware/software supply or storage rooms) must be constructed so that they are protected against fire, water damage, vandalism, and other threats known to occur, or that are likely to occur at the involved locations.

8. Security Incident Response Plan

8.1. All suspected information security incidents will be reported to the Information Technology Manager via management.

8.2. The Information Technology Manager will investigate all suspected incidents and report back to management.

8.3. When an information security incident occurs the Information Technology Manager will:

8.3.1. Assemble a team, as appropriate, to deal with the immediate threat or concern. The Team might consist of the Security Manager for the affected system, members of the Information Technology Office, and external sources such as the affected system vendor, Symantec or Microsoft Tech Support.

Acceptable Use Addendum

1. Internet/Intranet Usage

1.1. This technology usage agreement outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed under this section, but there is no right to privacy in an employee's use of the Internet/Intranet.

1.2. Use of the Internet, as with use of all technology resources, should conform to all City policies and work rules. Filtering software will be actively used by the City to preclude access to inappropriate web sites unless specific exemptions are granted as a requirement of work duties (e.g., police have the ability to access sites on criminal activity, weapons etc.). Attempts to alter or bypass filtering mechanisms are prohibited.

1.3. Except for City business related purposes, visiting or otherwise accessing the following sites is prohibited:

a. "adult" or sexually-oriented web sites
b. sites associated with hate crimes, or violence
c. sites that would create discomfort in a reasonable person in the workplace
d. Internet chat rooms, blogs and interactive website communication
e. personal dating sites
f. gambling sites

1.4. Staff violating this policy or otherwise engaging in inappropriate use of the Internet is subject to disciplinary actions up to and including termination from employment.

2. E-Mail Usage

2.1. E-mail content must comport with the same standards as expected in any other form of written (or verbal) communication occurring in a business setting where documents are subject to public disclosure.

2.2. Users must manage their e-mail in accordance with record retention policies and procedures as defined and identified by the City Clerk's Office.

2.3. Messages that must be retained are to be stored to alternative locations (like your Outlook Personal Folders). Retention of personal email should be minimized, and no restores or IT resources will be engaged to recover personal email "lost" in City systems.

2.4. Use of the "City Employees" distribution list is restricted to the City Mayor's Office, Department Directors and their specific designees. Under no circumstances should an employee "Reply to All" to an "City Employees" e-mail.

2.5. Users should be attentive to emails that have unusual or questionable subject lines to mitigate spam, phishing and script born viruses that come into the network through email attachments or by clicking on links that lead to hostile web sites. If you suspect phishing or script born viruses in email attachments immediately contact the IT Office.

2.6. The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening, and having not legitimate or lawful purpose or contents falling within the inappropriate categories for internet usage is prohibited.

2.7. Staff e-mail usage in violation of this policy or otherwise inappropriate e-mail usage is subject to disciplinary actions up to and including termination.

3. Network Access and Usage

3.1. Personal software or devices may not be loaded or attached to any City-owned equipment. The use of personal routers and wireless access points on the city network is not allowed.

3.2. Exploiting or attempting to exploit any vulnerability in any application or network security is prohibited. Sharing of internal information to others that facilitates their exploitation of a vulnerability in any application or network security is also prohibited. It is also prohibited to knowingly propagate any kind of spyware, denial of service attack, or virus onto the City network or computers. If you encounter or observe a vulnerability in any application or network security, report it to the IT Office immediately.

3.3. Disabling, altering, over-riding, turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden.

3.4. Because of band-width limitations inherent in any network system, use of the City network to download ***non-business*** related information is prohibited. Examples include, but are not limited to: streaming video of baseball games, streaming audio of radio programs, MP3 files, and on-line games.

3.5. Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to employees and the City of Issaquah.

End User Agreement

By signing this End User Agreement, I _____ (print name) agree to abide by the terms and conditions outlined in the Acceptable Use Addendum of Technology Resource Usage & Security Policy.

_____ _____

Employee Signature Date

Personal Smart Phone Usage

The Acceptable Use Addendum to IAM 101-26 prohibits connecting personally owned equipment to the city network. Personally owned smart phones (email-capable mobile phones) are increasingly being used by staff to access City email.

The security and integrity of City data and equipment necessitates managing how these personal smart phones are used to access the City email system.

Beginning January 1, 2012, all personal smart phone connections to the City email system must meet the following requirements (current phones not meeting the requirements are grandfathered until December 31, 2012):

- Department Head approval
- Not use a native phone email client, but instead be configured with the Microsoft Outlook mobile application and use no other means to access the City email system
- Have a remote data-wipe capability in case device is lost
- Allow a local passphrase, password, or PIN to be set to protect City data residing on the device
- Allow enforcement of passphrase/password/PIN compliance to limit work-arounds that compromise data protection

Important to Note:

- Accessing city email from personal devices must be only from the following methods:
    - Smartphones or Tablets – Only use Office365 application downloaded from iTunes or Android Play store.
    - PCs or Laptops – Only use Office365 web access (https://outlook.office365.com/mail/inbox).
    - Use of local Outlook or other email apps to access city email from personal devices is prohibited.
- Leaving City employment will require the Outlook application to be wiped.
- Lost or stolen phones will be remotely wiped of City email on the Outlook application.
- Employees using smart phones to access the City email system must promptly report lost or stolen phones to the IT Office by calling 425-837-3396 as soon as the loss is noticed regardless of time, day or night.
- While personal phones meeting the above standards may be used to access City email, the City is not responsible for troubleshooting personally-owned devices or instructing staff on how to use them.
- Be aware that using a personal smart phone for City business may result in personal records being subject to public disclosure and/or disclosure during litigation.
- For Personal smart phone connections to the City email system, Outlook calendar items and emails (received and responded to) will be retained through the Barracuda Email Archiver. Personal calendar applications and email accounts will not be.
- Text messaging related for city business is NOT appropriate. (Text messages are NOT retained as the texting component on personal smart phones is NOT connected to the City system.)

Department Head Approval (For Personal Smart Phone Access to City Email System)

Employee Printed Name, Signature and Date